Habilitación de funciones DHAP ESA

Contenido

Introducción

Este documento describe cómo habilitar la función de prevención de ataques de recolección de directorios (DHAP) en Cisco Email Security Appliance (ESA) para evitar ataques de recolección de directorios (DHA).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- ESA de Cisco
- AsyncOS

Componentes Utilizados

La información de este documento se basa en todas las versiones de AsyncOS.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Antecedentes

Un DHA es una técnica que utilizan los spammers para localizar direcciones de correo electrónico válidas. Hay dos técnicas principales que se utilizan para generar las direcciones que DHA apunta:

- El spammer crea una lista de todas las combinaciones posibles de letras y números y, a continuación, agrega el nombre de dominio.

- El spammer utiliza un ataque de diccionario estándar con la creación de una lista que combina nombres, apellidos e iniciales comunes.

El DHAP es una función soportada en los Cisco Content Security Appliances que se puede habilitar cuando se utiliza la validación de aceptación del Protocolo ligero de acceso a directorios (LDAP). La función DHAP realiza un seguimiento del número de direcciones de destinatarios no válidas de un remitente determinado.

Una vez que un remitente supera un umbral definido por el administrador, se considera que el remitente no es de confianza y el correo de ese remitente se bloquea sin necesidad de requisitos de diseño de red (NDR) ni generación de código de error. Puede configurar el umbral en función de la reputación del remitente. Por ejemplo, los remitentes no confiables o sospechosos pueden tener un umbral DHAP bajo y los remitentes confiables o confiables pueden tener un umbral DHAP alto.

Activar DHAP

Para habilitar la función DHAP, navegue hasta **Políticas de correo > Tabla de acceso de host (HAT)** desde la GUI del Dispositivo de seguridad de contenido y seleccione **Políticas de flujo de correo**. Elija la política que desea editar en la columna **Nombre de Política**.

HAT tiene cuatro reglas básicas de acceso que se utilizan para actuar sobre las conexiones de los hosts remotos:

- **ACCEPT (Aceptar):** Se acepta la conexión y la aceptación del correo electrónico está restringida aún más por la configuración del receptor. Esto incluye la Tabla de Acceso de Destinatarios (para receptores públicos).
- **RECHAZAR**: La conexión se acepta inicialmente, pero el cliente que intenta conectarse recibe un saludo 4XX o 5XX. No se acepta ningún correo electrónico.
- **TCPREFUSE**: La conexión se rechaza en el nivel TCP.
- **RELAY:** Se acepta la conexión. La recepción de cualquier destinatario está permitida y no restringida por la Tabla de acceso de destinatarios. La firma de claves de dominio sólo está disponible en las directivas de flujo de correo de retransmisión.

En la sección **Límites de flujo de correo** de la política seleccionada, busque y establezca la configuración de **Prevención de ataques de recolección de directorios (DHAP)** estableciendo el valor Máx. Destinatarios no válidos por hora. También puede optar por personalizar el máximo. Destinatarios no válidos por código de hora y máx. Texto de destinatarios por hora no válido si lo desea.

Debe repetir esta sección para configurar DHAP para políticas adicionales.

Asegúrese de enviar y confirmar todos los cambios en la GUI.

> **Nota:** Cisco recomienda que utilice un número máximo entre cinco y diez para la configuración **Número máximo de destinatarios no válidos por hora desde un host remoto**.

> **Nota:** Para obtener información adicional, consulte la **Guía del usuario de AsyncOS** en el portal de soporte de Cisco.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).